REMARKS

I. OVERVIEW

Claims 1, 8, 16, 17, 19, 20, 22, 25, 27, 28, 42, 43, 50, 51, 53, 54, 56, 61, and 68-71 are pending in the present application. No claims have been added by way of this current response. Claims 1 and 42 have been amended to more particularly recite the invention. Applicants respectfully note that per Examiner Subramanian's request, the present Supplemental Amendment shows all claim amendments made to the application as it existed on 31 August 2010. Accordingly, the amendments filed on 23 June 2011 and 04 August 2011 are each irrelevant.

II. INTERVIEW

Applicants would like to thank Examiner Subramanian for his assistance during the telephone interview held on April 19, 2011 and again during a conversation on 09 September 2011 regarding non-compliant amendments. During the telephone interview, the undersigned and Examiner Subramanian discussed the current state of the claims and different readings of the cited art. Although no agreement was reached, Applicants wish to express gratitude to Examiner Subramanian for his time and insight.

III. STATUS OF CLAIMS

Allowed Claims:	No claims have been allowed.
Withdrawn Claims:	No claims have been withdrawn.
Cancelled Claims:	Claims 2-7, 9-15, 18, 21, 23, 24, 26, 29-41, 44-49, 52, 55, 57-60, 62-67 were previously cancelled.
Pending Claims:	Claims 1, 8, 16, 17, 19, 20, 22, 25, 27, 28, 42, 43, 50, 51, 53, 54, 56, 61, 68, 69, 70, and 71 are pending in this application and stand finally rejected by the Examiner.

IV.   STATUS OF AMENDMENTS

Claims 1 and 42 are amended by the instant Response and Amendment to more particularly and clearly recite the claimed invention.

V.   SUMMARY OF THE CLAIMED SUBJECT MATTER

The present invention as set forth in independent claims 1 and 42 provides methods and systems for securely authorizing and transacting specific processing requests for stored-value cards from an originating merchant location over an originating communications network.[1]

Independent Claim 1

As recited in independent claim 1, a computerized method for securely authorizing and transacting specific processing requests for stored-value cards from an originating merchant location over an originating communications network,[2] the method comprising: storing in a database coupled to a central processor a plurality of records comprising information identifying specific merchant locations, if any,[3] and information identifying specific communications networks for carrying or transmitting stored value card processing requests, if any, including the originating communication network, that are authorized to transact specific processing requests, each of the specific merchant locations and the specific communications networks identified by an identifier;[4] receiving at the central processor a specific processing request for a stored-value card, along with the identifier of the originating merchant location or the originating communication network;[5] determining at the central processor whether the received identifier of the originating merchant location or the originating communication network is stored in the

---

[1] See, e.g., Abstract, paragraphs [0026] – [0038].
[2] See, e.g. Abstract, paragraphs [0008], [0026].
[3] See, e.g. Paragraph [0026].
[4] See, e.g. Paragraphs [0026], [0030].
[5] See, e.g. Paragraphs [0033] – [0034].

10

database as a trusted source for making the specific processing request;[6] responsive to a determination that the received identifier is associated with a trusted merchant location that is stored in the database as a trusted source for making the specific processing request, performing the specific processing request; [7] responsive to a determination that the received identifier is associated with a trusted communication network for making the specific processing request for the stored value card:[8] performing the specific processing request;[9] and capturing an identifier of the originating merchant location from which the specific processing request was sent over the originating communications network, deeming that the originating merchant location is a trusted source based upon its use of a trusted communications network, and storing the captured identifier of the originating merchant location in the database as a trusted merchant location for future processing requests, if not already stored in the database.[10]

Independent Claim 42

As recited in independent claim 42, a system for authorizing and transacting specific processing requests for stored-value cards from an originating merchant location over an originating communications network,[11] comprising: a database;[12] a storage module connected to the database and configured to store in the database a plurality of records comprising information identifying specific merchant locations, if any,[13] and information identifying specific communications networks for carrying or transmitting stored value card processing requests, if any,[14] that are authorized to transact specific processing requests for a stored value card, each of the specific

---

[6] *See, e.g.* Paragraphs [0036] – [0038].
[7] *See, e.g.* Paragraph [0038].
[8] *See, e.g.* Paragraph [0039].
[9] *See, e.g.* Paragraph [0039].
[10] *See, e.g.* Paragraphs [0042] – [0044].
[11] *See, e.g.* Abstract, paragraphs [0008], [0026].
[12] *See, e.g.* Paragraph [0026].
[13] *See, e.g.* Paragraph [0026].
[14] *See, e.g.* Paragraph [0030].

merchant locations and specific communications networks associated with an identifier;[15] a processing module in selectable communication with the database and storage module,[16] the processing module configured to: process a request from the originating merchant location to the processing module the request comprising an identifier of the originating merchant location or the originating communication network, the processing module configured to perform the request based on whether the received identifier is stored in the database as a trusted source for making the specific processing request for the stored value card;[17] and responsive to a determination that the received identifier is associated with a trusted merchant location that is stored in the database as a trusted source for making the specific processing request for the stored value card, performing the specific processing request for the stored value card;[18] responsive to a determination that the received identifier is associated with a trusted communication network for making the specific processing request for the stored value card:[19] performing the specific processing request for the stored value card;[20] and capturing an identifier of the originating merchant location from which the specific processing request was sent over the originating communications network, deeming that the originating merchant location is a trusted source based upon its use of a trusted communications network, and storing the captured identifier of the originating merchant location in the database as a trusted merchant location for future stored-value card processing requests.[21]

VI.   GROUNDS OF REJECTION TO BE REVIEWED

The grounds of Rejection are as follows:

---

[15] *See, e.g.* Paragraphs [0026], [0030].
[16] *See, e.g.* Paragraph [0038].
[17] *See, e.g.* Paragraphs [0036] – [0038].
[18] *See, e.g.* Paragraph [0042] – [0044].
[19] *See, e.g.* Paragraph [0038].
[20] *See, e.g.* Paragraph [0042].
[21] *See, e.g.* Paragraphs [0042] – [0044].

1. Whether all pending claims (1, 8, 16, 17, 19, 20, 22, 25, 27, 28, 42, 43, 50, 51, 53, 54, 56, 61, and 68-71) are properly rejected under 35 U.S.C. § 112, second paragraph as being allegedly indefinite for failing to particularly point out and distinctly claim the subject matter Applicants regard as the invention.

2. Whether all pending claims (1, 8, 16, 17, 19, 20, 22, 25, 27, 28, 42, 43, 50, 51, 53, 54, 56, 61, and 68-71) are properly rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,903,633 to Lorsch ("Lorsch") in view of U.S. Patent No. 6,381,631 to Van Hoff ("Van Hoff").

VII. ARGUMENTS

Applicants respectfully submit that the rejections against the pending claims in the instant application should be reversed for at least the reasons below.

The rejection under 35 U.S.C. 112, second paragraph is moot in view of the present amendment. The present amendment removes the "may include" language objected to by the Examiner. Accordingly, the rejection of all pending claims (claims 1, 8, 16, 17, 19, 20, 22, 25, 27, 28, 42, 43, 50, 51, 53, 54, 56, 61, 68, 69, 70 and 71) under 35 U.S.C. 112, second paragraph, should be withdrawn.

Applicants submit that all pending claims (1, 8, 16, 17, 19, 20, 22, 25, 27, 28, 42, 43, 50, 51, 53, 54, 56, 61, and 68-71) are improperly rejected under 35 U.S.C. § 103(a) over Lorsch in view of Van Hoff. Appellants respectfully submit that this rejection is improper because the Office fails to set forth a *prima facie* case of obviousness. Independent claims 1 and 42 stand or fall together. Independent claim 1 will be used as a representative claim. Appellants submit that the rejection of claim 1 under 35 U.S.C. § 103(a) is improper because the references, if properly combined, fail to teach or suggest all of the recited claim limitations.

The Present Invention Seeks to Determine if a
Transaction Request Comes from a Trusted Source

The present invention looks to provide systems and methods for determining if a requested transaction for a stored value card should be permitted, at least in part by determining if the transaction request comes from a trusted source. *See, e.g.*, paragraph [0026]. Among other things, the present invention identifies at least two characteristics of trusted sources – merchant locations and/or communication networks. *See, e.g.*, paragraph [0026]. The invention determines if an identifier captured from the originating or requesting merchant location is stored as a trusted identifier in a database. *See, e.g.*, paragraph [0026] – [0028]. The invention further determines if the transaction request is received over a communications network that is considered trusted. *See, e.g.*, paragraphs [0030], [0036]. If the communications network is trusted, then the identifier of the merchant location is captured and added to the database of trusted locations. *See, e.g.*, paragraphs [0038], [0042].

Looking to the precise claim language, claim 1 of the present invention explicitly recites these steps. Claim 1 determines if the merchant location is trusted, reciting "determining at the central processor whether the received identifier of the originating merchant location or the originating communication network is stored in the database as a trusted source for making the specific processing request for the stored value card." Claim 1 determines if the communication network is trusted, reciting "responsive to a determination that the received identifier is associated with a trusted communication network for making the specific processing request for the stored value card: performing the specific processing request for the stored value card." Following a determination that the communication network is trusted, the claim then teaches "capturing an identifier of the originating merchant location from which the specific processing request was sent over the originating communications network, deeming that the originating merchant location is a trusted source based upon its use of a trusted communications network, and storing the captured identifier of the originating merchant location in the database as a trusted merchant location for future stored-value card processing requests."

Lorsch Fails to Disclose or Teach All Recited Claim Elements

Applicants respectfully submit that Lorsch fails to disclose, teach, or suggest each of the recited and required claim elements.

Lorsch Teaches Authorizing Activation Based Upon Terminal Identity

Lorsch relates to prepaid phone card activation, and discloses the use of information read from a phone card, information stored in a centralized database, and information from a point of sale terminal to determine whether an activation attempt is authorized. Lorsch at 1:9-12; 7:28-37.

> The above information may then be processed and compared to information regarding the specific PIN that is already in the centralized database. Specifically, software will compare the information provided by the point of sale terminal to determine if the location of the point of sale terminal where the card is being swiped matches the client that is identified by the control code that is encoded on the magnetic strip of the card. This comparison is described in more detail in the detailed description, below. If the computer determines that the card was swiped through an authorized terminal at the correct client, then the PIN associated with that card may be activated, so that calls can be made using that card and PIN. At this point, the computer may return a code or message to the point of sale terminal, in much the same way that an approval code is sent at the end of a credit card transaction, confirming that the activation process was finished and the card is now usable. This code may consist of the last few digits of the PIN code or the control code, which may be completely or partially exposed on the card.

Lorsch discloses a centralized database relating prepaid phone cards, merchants, and terminals. The centralized database maintains records of merchants authorized for specific cards, as well as terminals belonging to those merchants. Lorsch at 3:46-65. When a prepaid phone card is swiped at a point of sale terminal belonging to the system contemplated by Lorsch, software compares a merchant identified by a control code encoded on a magnetic strip of the card with information provided by the terminal, in order to determine whether the terminal is at a location matching the merchant. Lorsch at 3:65. If the software determines that the card was swiped through a terminal at the correct merchant, the PIN associated with the prepaid phone card is activated.

It can be seen above that Lorsch merely captures information from the point of sale terminal requesting the activation, and determines if there is an association between (a) the requesting terminal and (b) the merchant with whom the stored value card is associated. Lorsch has no suggestion, disclosure, or teachings related to the specific claim elements recited by the invention.

Lorsch Does Not Disclose the Recited Claim Elements

Specifically, Lorsch fails to disclose, teach, or suggest the recited claimed elements of:

(i)   "[D]etermining at the central processor whether the received identifier of the originating merchant location or the originating communication network is stored in the database as a trusted source for making the specific processing request for the stored value card."

(ii)   "[R]esponsive to a determination that the received identifier is associated with a trusted communication network for making the specific processing request for the stored value card: performing the specific processing request for the stored value card."

(iii)   "[C]apturing an identifier of the originating merchant location from which the specific processing request was sent over the originating communications network, deeming that the originating merchant location is a trusted source based upon its use of a trusted communications network, and storing the captured identifier of the originating merchant location in the database as a trusted merchant location for future stored-value card processing requests."

Moreover, Lorsch fails to (1) use identifiers of a terminal or point of sale location to determine if a requested transaction is authorized; (2) use identifiers of a location or communications network to determine – *after connected* – whether the specific requested transaction is authorized; and (3) use a *network* as an indicator of the trustworthiness of a merchant location, and based upon the *network*, considering and recording the merchant location as a trusted source.

Van Hoff Does Not Cure the Deficiencies of Lorsch

Van Hoff is directed to a process for authenticating a user and/or a network. Either (i) a network must be authenticated before a user can connect to it; or (ii) a user must be authenticated before the user can connect to the network. Van Hoff, col. 8, lines 49-57; col. 11, lines 4-37. Van Hoff merely teaches determining whether or not to connect to a network. Van Hoff also teaches maintaining a trusted network list by a third party. If a network is present on the trusted network list, a user will be permitted to connect to the network.

Van Hoff fails to disclose, teach or suggest at least the claim elements of:

(i) "[D]etermining at the central processor whether the received identifier of the originating merchant location or the originating communication network is stored in the database as a trusted source for making the specific processing request for the stored value card."

(ii) "[R]esponsive to a determination that the received identifier is associated with a trusted communication network for making the specific processing request for the stored value card: performing the specific processing request for the stored value card."

(iii) "[C]apturing an identifier of the originating merchant location from which the specific processing request was sent over the originating communications network, deeming that the originating merchant location is a trusted source based upon its use of a trusted communications network, and storing the captured identifier of the originating merchant location in the database as a trusted merchant location for future stored-value card processing requests."

In addition to the omitted claim recitations discussed above, Applicants respectfully submit that while the Office asserts (assuming, *in arguendo* that the Office is correct) that Lorsch discloses authorization based upon terminal identifiers, and that Van Hoff discloses authorization using identifiers of network identity – and maintaining a list of networks that are authorized. However, neither reference – taken alone or in combination – teach the use a ***network*** as an indicator of the trustworthiness of a merchant location, and based upon the ***network***, considering and recording the merchant location as a trusted source. Nor is it proper to consider it obvious to combine

17

these references to disclose such aspects of the invention. Any efforts do so would be solely based upon impermissible hindsight.

Accordingly, Appellants respectfully request withdrawal of the rejection of claim 1 under 35 U.S.C. § 103(a) as being unpatentable over Lorsch in view of Van Hoff.

Independent claim 42 includes the same limitations as those discussed above with regard to claim 1. Accordingly, Applicants respectfully request withdrawal of the rejection of claim 42 under 35 U.S.C. § 103(a) as being unpatentable over Lorsch in view of Van Hoff.

Claims 8, 16, 17, 19, 20, 22, 25, 27, 28, 61, 68, 69, 70 and 71 depend off of independent claim 1, which has been shown above to be patentable over Lorsch in view of Van Hoff. Claims 43, 50, 51, 53, 54, and 56 depend off of independent claim 42, which has been shown above to be patentable over Lorsch in view of Van Hoff on the same grounds as claim 1. Accordingly, Applicants respectfully request that the Office withdraw the rejections of claims 8, 16, 17, 19, 20, 22, 25, 27, 28, 43, 50, 51, 53, 54, 56, 61, 68, 69, 70 and 71 under 35 U.S.C. 103(a) as being allegedly unpatentable over Lorsch in view of Van Hoff.
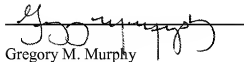
VIII.   CONCLUSION

For all the reasons set forth above, it is respectfully submitted that all outstanding rejections have been overcome.   All pending claims 1, 8, 16, 17, 19, 20, 22, 25, 27, 28, 42, 43, 50, 51, 53, 54, 56, 61, and 68-71 are patentably distinct over the prior art of record. Appellants accordingly submit that these claims are in condition for allowance. Reconsideration and allowance of all claims is respectfully requested.

Should the Office have any questions or wish to discuss the present application, please contact the undersigned representative of Applicants at the number listed below.

September 13, 2011

By:

Gregory M. Murphy
Reg. No. 52,494
(E)   gmurphy@LandmarkIP.com
(T)   804.971.7729
(F)   804.767.3416

* * * *

Please Direct all Correspondence to:

LANDMARK INTELLECTUAL PROPERTY LAW, PLLC
19925 Stevens Creek Blvd, Suite 100
Cupertino, California 95014
info@LandmarkIP.com